APPENDIX 3
GENERIC SWITCHING CENTER REQUIREMENTS (GSCR) 08 SEP 03
DSN VOICE OVER INTERNET PROTOCOL (VOIP) REQUIREMENTS

Phase 1

A3.1 Background

This appendix describes the requirements that will be used to certify Voice over Internet Protocol (VoIP) Phase 1 for Defense Switched Network (DSN) applications. Where conflicts between this appendix and the body of the GSCR arise, the GSCR body takes precedence. This appendix applies to both converged and non-converged networks, but does not address the impact of prioritized voice on data applications and video services. This appendix addresses a wired LAN, but does not address wireless LANs. In addition, the appendix does not address how VoIP should be implemented in the presence of firewalls. Finally, the appendix does not address migration strategies for legacy systems and approaches for integrating VoIP with an existing C/P/S infrastructure. Future revisions of this appendix may address these voids based on the customer and industry feedback. The requirements contained in this appendix are based on:

a. Policy for DOD voice networks as outlined in the Chairman of Joint Chiefs of Staff Instruction (CJCSI) 6215.01B, "Policy for Department of Defense Voice Networks."

b. The Defense Information Systems Agency (DISA), Joint Interoperability and Engineering Organization (JIEO), Technical Report 8249, "Defense Information Systems Network (DISN) Circuit Switched Subsystem, Defense Switched Network (DSN) Generic Switching Center Requirements (GSCR)," March 1997.

c. Global Information Grid (GIG) Capstone Requirements Document (CRD).

d. DISA, NS533, "GSCR," 08 September 2003 (draft).

CJCSI 6215.01B defines the DSN as being "an interbase non-secure/secure or C2 telecommunications system that provides end-to-end command use and dedicated telephone service, voice-band data, and dial-up VTC for C2 and non-C2 DOD authorized users in accordance with national security directives." The CJCS instruction further specifies the need for the DSN to offer military unique features (MUFs) such as Multi-level Precedence and Preemption (MLPP) and military Network Management (NM).

DISA has been delegated the authority for both system management and engineering of the DSN. The requirements for certification of DSN switching systems are outlined in the GSCR document. Certification of switching systems by the Joint Interoperability Test Command (JITC) is primarily based on the GSCR. For use within the DSN, systems will be certified in accordance with their placement within the DSN architecture: Tandem Switch (TS), Multifunction Switch (MFS), End Office (EO), Small End Office (SMEO), Private Branch Exchange 1 (PBX 1) - with MLPP and PBX 2 - without MLPP. This appendix deals with the requirements for the following Phase 1 VoIP systems:

a. Command and Control Voice Grade LAN (C2VGLAN), i.e., one capable of supporting MLPP and used in MFS, EO, SMEO, and PBX1 applications.

b. Voice Grade LAN (VGLAN), i.e., a non-C2 LAN for PBX2 applications.

VoIP implementation within the DSN will take place in two major phases:

a. Phase 1 involves IP islands interconnected via the traditional DSN, which consists of circuit-switched systems and TDM transmission facilities. As such, the existing non-IP systems provide for the standardized interoperability between various IP-based systems.

b. Phase 2 involves full network-wide IP interoperability and replaces the traditional circuit-switch and TDM technology.

This version of Appendix 3 only addresses Phase 1.

A3.1.1 Definitions

a. C2 VGLAN. The C2VGLAN is defined as the IP network infrastructure components used to provide C2 voice services to an IP telephony subscriber. It applies to switch certifications for MFS, EO, SMEO and PBX1.

b. Converged Network. An IP network used to transmit a combination of voice, video, and/or data services. The converged definition applies to a singular camp, post or station IP network that will be used to provide IP services along with the addition of DSN VoIP services.

c. Internet Protocol (IP) Centric. IP centric architectures are designed around an IP core packet switching system. These solutions have distributed IP devices that function together to perform the functions of a circuit switch as shown in Figure 1. For IP centric solutions, the connectivity to the rest of the DSN architecture shall be via the interfaces mandated by the GSCR, e.g., Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) or Signaling System 7 (SS7), not IP. IP centric solutions shall be tested IAW the GSCR for specific switch type applications.

Initially, analog phones, STE and STU instruments, facsimile devices, video equipment, and modems may terminate directly on the VoIP Gateway, as shown in Figure 1. However, future versions of this appendix will require these devices to terminate on an IP access device (IAD) connected to an Ethernet access switch in order to connect to the VoIP Gateway.

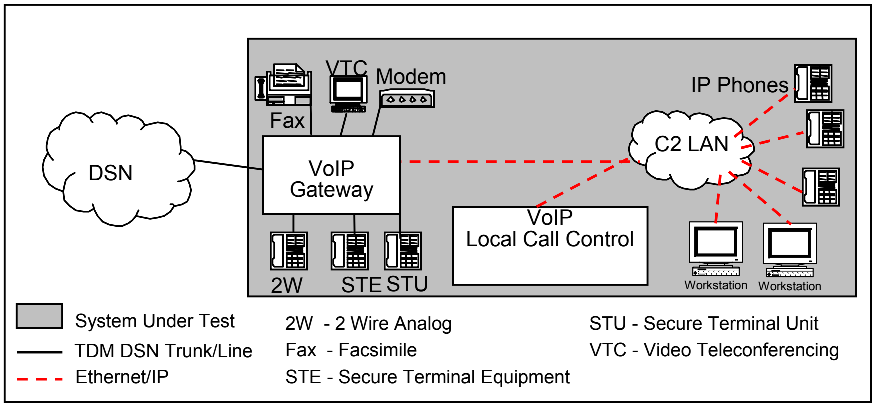


Figure 1. Depiction of IP Centric Architecture

d. IP enabled. The IP enabled approach utilizes traditional time division multiplexing (TDM) circuit switches that offer VoIP as a line instrument. This solution has a TDM circuit switch as the core device with VoIP being provided as a line function similar to other analog or digital telephony instruments as shown in Figure 2. The requirements of the GSCR for non-secure/secure voice, data, VTC and facsimile are primarily met via the circuit switch portion. The DSN interface requirements (T1/E1, etc) are provided via the circuit switch and the connectivity to the IP LAN is via Ethernet. IP enabled architectures can be certified for PBX through MFS applications. A VoIP Gateway is not shown in Figure 2 because it is usually built into the TDM circuit switch.

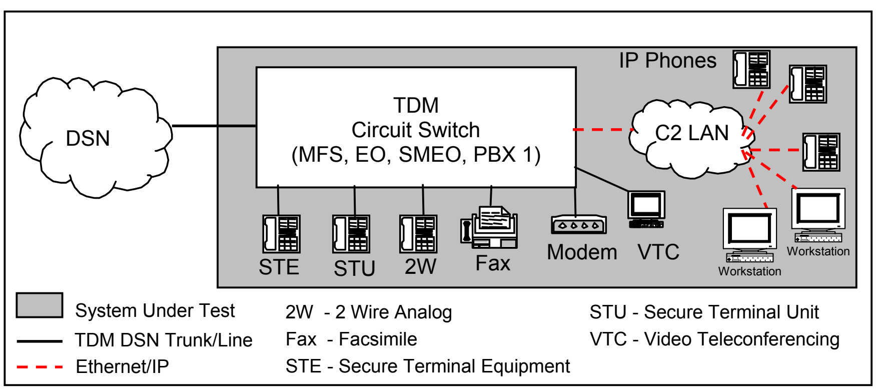


Figure 2. Depiction of IP Enabled Architecture.

e. IP Telephony subscriber. A DSN C2 or non-C2 user that receives voice service via an IP telephone instrument.

f. IP Data User. A user connected to an IP network to receive DOD IP services such as data and IP video; DSN IP telephony is not included.

g. LAN Network Links. Network links are defined as those internal IP/Ethernet links that interconnect LAN components.

h. Link Pair. To ensure no single point of failure to more than 64 IP telephony subscribers, IP network links shall have a second link (standby or load sharing). The combination of the two links is called a 'link pair'

i. Non-blocking LAN. Within the C2VGLAN, all provisioned IP phone instruments can be simultaneously off hook and successfully engaged in a full duplex voice call.

j. Non-converged Network. A non-converged network is defined as being a network that is used solely to provide DSN VoIP services. A separate IP network will be used to provide IP data services.

k. SUT. The system under test (SUT) is defined as the inclusive components required to meet a DSN switch certification (i.e., MFS, EO, etc.). Examples of a SUT are TDM or circuit switch components, VoIP system components (e.g., local call controller and gateway), LAN components (e.g., routers and Ethernet switches), and end instruments.

l. Trunks. Trunks are defined as being the Time Division Multiplexing links used by a circuit switch or VoIP system to connect to or interconnect DSN switches.

m. VGLAN. The Voice Grade LAN is defined as the IP network infrastructure required to provide non-MLPP IP voice services. The VGLAN applies only to PBX 2 switch certifications.

n. VoIP System. A VoIP system is defined as those components required to provide DSN IP voice services from end instrument to DSN trunk, or IP phone to IP phone. The VoIP system includes but is not limited to: the IP telephony instrument, LAN, local call controller, and IP gateway.

A3.1.2 Approach

The requirements contained within this appendix are a supplement to the main body of the GSCR to address VoIP unique requirements. The SUT will be required to meet the pertinent GSCR requirements defined for each of the switch types. For VoIP systems that wish to be certified to provide switching systems functions, in addition to the GSCR switching system requirements, the VoIP system requirements and appropriate IP LAN (C2VGLAN or VGLAN) requirements contained within this appendix also apply. The requirements nomenclature used within this appendix is consistent with the main body of the GSCR with the addition of LAN applicability. Paragraphs may caveat requirements that apply specifically to converged versus non-converged LANs. Requirements specified for C2VGLAN and VGLAN are meant to apply to both converged and non-converged LANs). Examples of nomenclature follow.

a. SUT applicability. Requirements that apply to be certified for switch type (MFS to PBX). **[REQUIRED: TS, EOS, MFS, SMEO, PBX1 - CONDITIONAL: PBX2]**.

b. LAN applicability. Requirements that are applicable to the LAN for both converged and non-converged applications used to distribute IP voice services. **[REQUIRED: C2VGLAN - CONDITIONAL: VGLAN]**.

c. Network type applicability. Those requirements that apply specifically to converged or non-converged networks. **[REQUIRED: C2VGLAN (converged) - CONDITIONAL: C2VGLAN (non-converged), VGLAN]**.

A3.1.3 Certification

IP solutions will be certified IAW the GSCR (08 September 2003) and this appendix. To be certified switching platforms shall meet the physical interface and feature/capability requirements. Current interface requirements by switch type are provided in Enclosure A. Feature/capability requirements by switch type are provided at Enclosure B. For VoIP solutions, this appendix contains LAN architecture examples that will be used in the DSN interoperability test certifications.

A3.1.3.1 IP Enabled

The same functionality received today by telephony subscribers, including MLPP, will be provided by IP enabled equipment. Since no approved standards exist for the provision of MLPP in an IP environment, vendors may temporarily provide proprietary solutions in order to meet the MLPP functionality. The ability of the equipment in the C2VGLAN to provide voice services IAW DOD requirements will be tested using JITC's Generic Switch Test Plan (GSTP) in conjunction with the circuit switch portion of the solution. Upon meeting the requirements, JITC will issue an appropriate letter of certification (e.g., MFS, EO, SMEO, PBX1, or PBX2) for the combined TDM & IP equipment.

A3.1.3.2 IP Centric

IP Centric solutions will be required to meet the current interfaces IAW the GSCR (Enclosure A). Current requirements for secure voice, secure/non-secure facsimile and video teleconferencing (VTC) shall also be provided by the IP Centric solution. To be certified for joint use, the IP Centric VoIP system will be required to interface to existing DSN circuit switches at the MFS, EO or SMEO level via an approved DSN interface type.

A3.2 VoIP System Requirements

A3.2.1 Voice Quality

[REQUIRED: TS, EOS, MFS, SMEO, PBX1, PBX2] For VoIP LAN systems used in DSN, the voice quality shall have a mean opinion score (MOS) of 4.0 or better, as measured in accordance with JTA voice quality standards. This applies from handset to handset, and from handset to gateway trunk to the DSN.

A3.2.2 Coder/Decoder (CODEC)

[REQUIRED: TS, EOS, MFS, SMEO, PBX1, PBX2] The term codec is an acronym for "coder/decoder" or is also sometimes known as "compressor/decompressor." The codec takes one format of audio signal and encodes it into some other digital format with an algorithm (i.e., the encoding). It also decodes the same data, reconstructing the format. The International Telecommunications Union Telecommunication Standardization Sector (ITU-T) has developed the G.7xx series of recommendations for codecs for different data rates and voice qualities. **For a VoIP LAN system used in the DSN, the G.711 Pulse-Code Modulation (PCM) codec shall be used. No voice compression technique of any type shall be used within the DSN.**

A3.2.3 Multi-level Precedence & Preemption (MLPP)

[REQUIRED: TS, EOS, MFS, SMEO, PBX1 - CONDITIONAL: PBX2] The VoIP telephony system shall meet all MLPP requirements identified in Section 3 of this GSCR. Therefore, the C2VGLAN shall also be capable of processing MLPP calls. Since no complete set of standards exists for MLPP over IP, vendors may initially implement proprietary protocols in the C2VGLAN to ensure the complete MLPP functionality as detailed in section 3 of the GSCR is provided to the DSN IP telephony subscriber.

A3.2.4 Security

[REQUIRED: TS, EOS, MFS, SMEO, PBX1, PBX2] With the advent of VoIP technology, the basic security requirements for all switches remains the same, but additional measures must be applied to secure the DSN from threats that predominately have been the domain of the data networks realm. The European Telecommunications Standards Institute, in conjunction with the ITU-T, have produced two documents describing the threats to the TIPHON (Telecommunications and Internet Protocol Harmonization over Networks) VoIP model, a general VoIP scenario, and described the countermeasures that can minimize the risk to VoIP systems to an acceptable level. The TIPHON scenario is a general model that applies to SIP, H.323, BICC, and other VoIP signaling and transport protocols. ETSI Technical Specification 102 165-1 (v4.1.1) provides a threat analysis for VoIP architectures, with specific reference to SIP and H.323 in Annexes A and B, respectively. This document describes the likelihood and potential impact of various threats to security services and describes the resulting risk factor for the various threats to VoIP. ETSI Technical Specification 102 165-2 (v4.1.1) provides a detailed description of countermeasures that, if implemented properly, can reduce the overall risk of operating a VoIP solution. The list of countermeasures includes authentication, access control, and confidentiality methods. The implementation of these methods can reduce risk. However, each countermeasure also introduces new threats to the system by adding complexity. In some instances a specific countermeasure cannot be applied to a particular technology. **All VoIP systems shall be designed and implemented in a way that acknowledges the possible threats to VoIP protocols and seeks to offer countermeasures to those threats were technically feasible**.

GSCR Appendix 3 - DSN VoIP Requirements

The following security requirements shall apply, as defined below for equipment employing VoIP.

All VoIP Systems, shall follow the DSN Switch Certification and Accreditation Processes as defined in Section 6, Procedures, of the Department of Defense Instruction (DoDI) 8100.XX, "Department of Defense (DoD) Voice Networks," dated xx/xx/03 (still pending signature), in completing the IA Certification requirement. A subdocument of the defined procedures in the DoDI 8100.XX process is the Information Assurance Test Plan (IATP). The DISA DSN VoIP IATP, dated July 2003, is the guideline in providing security features test criteria for telecommunications switches connected or planned for connection to the DSN. The IATP will evaluate security features within the existing network and critical areas involving MUF and new telecommunications technology. The IATP will also address security features between new technologies; new technologies and the existing network; and the performance impact of these new technologies on MUF. The IA testing will be conducted and the system secured in accordance with the applicable Security Technical Implementation Guides (STIGs), prior to operation of telecommunications switches connected to the DSN.

Additionally, DSN switching platforms require accreditation prior to being authorized connectivity to the DSN in accordance with the Draft DoDI 8100.XX and DoDI 5200.40 "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP),", dated 30 December 1997. **VoIP systems shall be required to be certified and accredited in accordance with the DITSCAP process.**

VoIP implementations within DoD for the provision of voice services shall meet the same stringent security procedures as circuit switches. VoIP systems, either IP Enabled or IP Centric, shall adhere to the GR-815-CORE security measures already outlined in Section 13 (Security) of this GSCR to provide the features and functionality needed to implement the requirements of the DSN Security Technical Implementation Guide (STIG). Additionally, the VoIP system shall provide the features and functionality needed to implement the requirements of the VoIP STIG, Draft, 15 September 2003, as pertaining to the VoIP System and its subcomponents, excluding the LAN requirements. LAN security requirements are defined in Section A.3.3.4.3 of this Appendix.

Any VoIP subcomponents that utilize OS/data client/Internet/network technologies (e.g., Windows XP, Windows 2000, Windows NT, Unix; DBMS/SQL Databases, Oracle, and/or Web Service) for which DISA Field Security Office (FSO) STIGS are enforced, the VoIP subcomponents shall provide the features and functionality needed to implement the requirements of the appropriate DISA FSO STIG requirements. Where there is a direct conflict of requirements between the OS/data client/Internet/network technologies subcomponent STIGs and the VoIP STIG, the VoIP STIG requirements shall take precedence. Where no conflicts exist in requirements, the features and functionality needed to implement the requirements of all STIGs shall apply simultaneously. See Figure 3 for the hierarchical precedence of STIG requirements.

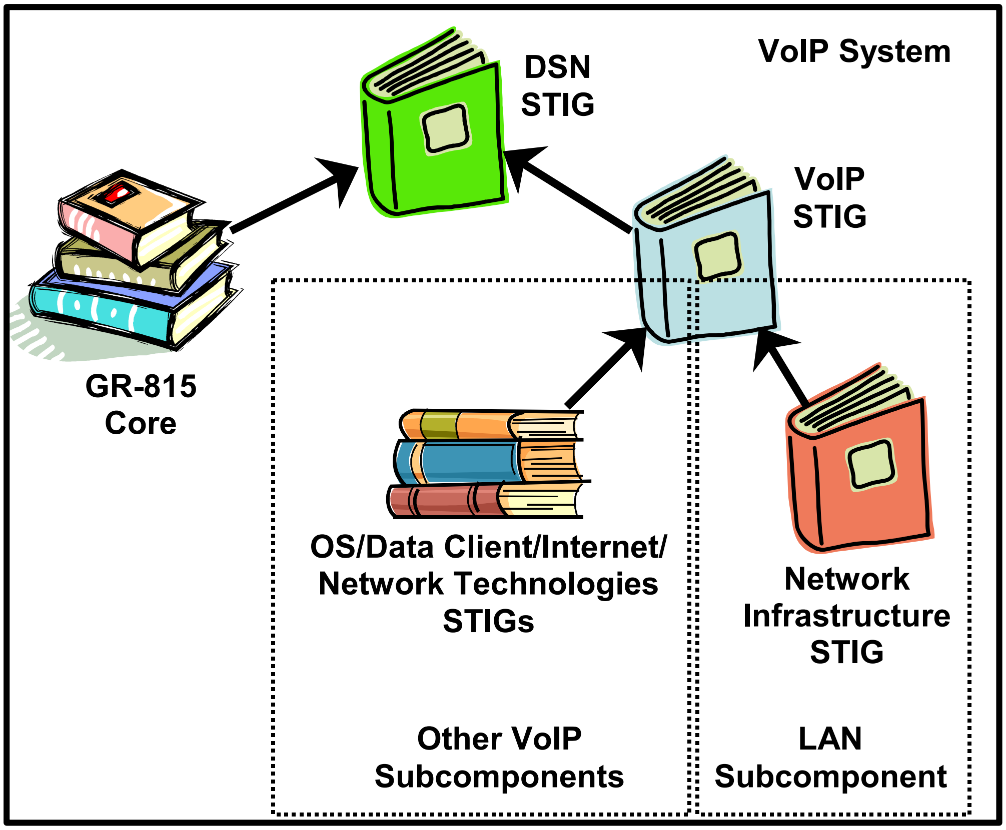


Figure 3. Hierarchical Precedence of STIG Requirements

A3.2.5 Network Management (NM)

[REQUIRED: TS, EOS, MFS, SMEO - CONDITIONAL: PBX1, PBX2] The VoIP system shall meet the NM functions described in Section 9 of this GSCR as applicable to switch type. LAN manageability functions specific to the LAN are described in section A3.3.4.2 of this appendix. NM requirements specific for the LAN may be provided via an additional interface above and beyond those NM interfaces required in Section 9.

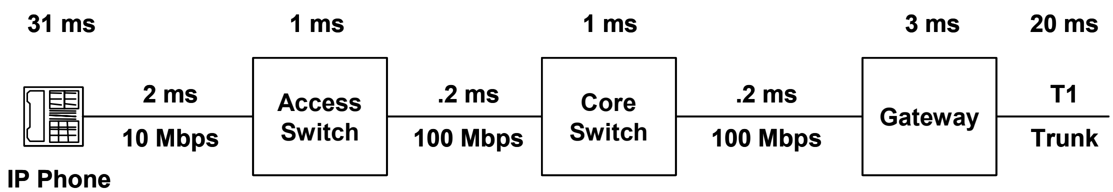
A3.2.6 Timing

[REQUIRED: TS, EOS, SMEO, MFS, PBX1, PBX2] The VoIP system shall support line timing modes as defined in GSCR, Section 11.1.1.2, Line Timing Mode.

[REQUIRED: TS, EOS, MFS - CONDITIONAL: SMEO, PBX1, PBX2] The VoIP system shall provide internal clock requirements as described in the Telcordia, GR-518-CORE, Issue 1, May 1994, paragraph 18.2.

A3.2.7 Latency

[REQUIRED: TS, EOS, MFS, SMEO, PBX1, PBX2] The one-way system latency for the SUT/VoIP system shall be 60 msec or less as averaged over any five-minute period. The latency is to be measured from IP handset to egress from the SUT via a DSN trunk. An illustrative reference circuit diagram for this specification is shown in Figure 4.



Dc – Codec Delay (31 ms) (G.711 with look ahead + PLC)
Ds – Serialization Delay (2 or .2 or 20 ms) (210 byte packets)
Dj – De-jitter Buffer Delay (1/2 delay variation, assume 3 ms)
Dp – Propagation Delay (negligible)
Dx – Switching Delay (assume 1 ms max.)
Dt – Total 1-way delay
Dt = Dc + Ds + Dx + Dp + Dj
Dt = 31 + 22.4 + 3 + 0 + 3 = 59.4 ms

Figure 4. LAN Delay from Mouth to Trunk to DSN Switch

A3.2.8 IPv6 Capable

[REQUIRED: TS, EOS, MFS, SMEO, PBX1, PBX2] All IP devices in the VoIP system shall be IPv6 capable (in addition to maintaining interoperability with IPv4 systems) in accordance with the JTA.

A3.3 Local Area Network (LAN) Requirements

There are several capabilities and characteristics that need to be addressed when implementing VoIP. The following are those capabilities and characteristics that are significant for DSN VoIP implementations:

a. LAN Parameters

1) Delay (Latency)

2) Jitter

3) Packet loss

b. Class of Service (CoS)

1) CoS models

2) Traffic Prioritization

c. Quality of Service (QoS)

1) Queuing

2) Policing

3) Virtual LANs (VLANs)

d. LAN Design

1) Reliability

2) Management

3) Security

4) Traffic Engineering

5) Architectures

A3.3.1 LAN Parameters

A3.3.1.1 Delay

[REQUIRED: C2VGLAN, VGLAN] Packet delay (latency) is the length of time it takes a packet to traverse the LAN. Each element of the network adds to packet delay, including Ethernet switches, routers, distance traveled through the network, firewalls, and jitter buffers**. The one-way packet delay for packets of an established call (signaling and media) within the LAN for a DSN VoIP system shall be 5 milliseconds (msec) or less as averaged over any five minute period.**

A3.3.1.2 Jitter

[REQUIRED: C2VGLAN, VGLAN] Jitter is defined as the statistical average variance in delivery time between packets or datagrams. Jitter is introduced by the variable transmission delay over the network. Removing jitter requires collecting packets and holding them long enough to allow the slowest packets to arrive in time to be played in the correct sequence, which causes additional delay. **For voice media packets jitter shall be 5 msec or less as averaged over any five minute period.** (Jitter is not a problem for signaling packets, since they do not occur in streams.)

A3.3.1.3 Packet Loss

[REQUIRED: C2VGLAN, VGLAN] Network packet loss occurs when packets are sent, but not received at the final destination. **LANs shall be engineered for a theoretical packet loss of zero for voice packets; actual or measured voice packet loss within the LAN shall not exceed 0.05% averaged over any five minute period.**

A3.3.2 Class of Service (CoS)

CoS is a mission-sensitive indication of relative 'priority' of an individual application session (e.g., phone call). CoS is determined by end user at time of session origination and is determined solely by mission content. CoS methods used within the DSN can be constrained by "class-mark" privileges and authentication. CoS is a classification method only; it does not ensure a level of Quality of Service (QoS), but is the method used by queuing mechanisms to limit delay and other factors to improve QoS.

Common CoS models include the IP TOS (Type Of Service) byte, Differentiated Services Code Point (DiffServ or DSCP, defined in RFC 2474 and others) and the Institute of Electrical and Electronic Engineers (IEEE) Inc 802.1p/Q. CoS, or tagging, is ineffective in the absence of QoS because it can only mark data. QoS relies on tags or filters to give priority to data streams.

A3.3.2.1 CoS Models

[REQUIRED: C2VGLAN (converged), VGLAN (converged) - CONDITIONAL: C2VGLAN (non-converged), VGLAN (non-converged)] For converged LANs, the traffic on the LAN is comprised of voice media streams, voice signaling, Operations, Administration & Maintenance (OA&M) packets, video and data packets. Converged LANs, shall support CoS.

For converged LANs, the routers and Ethernet switches shall support 802.1p to DSCP mapping and at least one of the following standards:

a. **Institute of Electrical and Electronic Engineers (IEEE) Inc. 802.1p/Q**. 802.1p is a specification for giving Layer 2 switches the ability to prioritize traffic (and perform dynamic multicast filtering). The prioritization specification works at the media access control (MAC) framing layer of the OSI model. 802.1p uses 802.1Q "tagged" bytes to distinguish classes of service. The 802.1Q specification also establishes a standard method for inserting virtual LAN (VLAN) membership information into Ethernet frames.

b. **DSCP**. DSCP is a part of the DiffServ framework specified by the Internet Engineering Task Force (IETF) in RFC 2474. DSCP is a six-bit field in an IP packet header from which as many as 64 classes of service can be created.

c. **IP TOS**. The TOS byte is in an IP header to prioritize traffic. TOS is an eight bit field comprised of which the first three bits is an IP Precedence portion that enables the creation of eight service classes, compared with the 64 classes possible in the DiffServ model.

A3.3.2.2 C2VGLAN Traffic Prioritization

[REQUIRED: C2VGLAN (converged), VGLAN (converged). CONDITIONAL: C2VGLAN (non-converged), VGLAN (non-converged)] Within the converged LAN different types of traffic are expected. The following is a listing of traffic streams prioritized from highest to lowest. Priorities shall be applied IAW the CoS models listed above.

a. Voice and Video Signaling and LAN Network Management (highest)

b. Voice and Video Media Stream

c. Data Traffic (lowest)

A3.3.3 Quality of Service (QoS)

QoS is defined as being the collection of technologies that allow applications/users to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter) and delay (i.e., it refers to the capability of a network to provide better service to selected network traffic). QoS involves giving preferential treatment through queuing, bandwidth reservation, or other methods based on attributes of the packet, such as CoS priority. A service quality is then negotiated. The following paragraphs (A3.3.3.1 through A3.3.3.3) outline the QoS requirements for the LAN in support of VoIP systems.

A3.3.3.1 Queuing

[REQUIRED: C2VGLAN (converged), VGLAN (converged) - CONDITIONAL: C2VGLAN (non-converged), VGLAN (non-converged)] For converged LANs, the routers shall support at least one of the following queuing mechanisms:

a. **Priority Queuing (PQ).** PQ supports some number of queues, usually from high to low. Queues are serviced in strict order of queue priority, so the high queue always is serviced first, then the next lower priority and so on. If a lower priority queue is being serviced and a packet enters a higher priority queue, that higher priority queue is serviced immediately after the current packet from the lower queue is sent. (Strict Priority Queuing cannot be used.)

b. **Custom Queuing (CQ).** CQ allows a network administrator to reserve a percentage of bandwidth for specified protocols. Custom queuing has a large number of queues and transmits a configurable amount of data from a queue before proceeding to the next. This queuing strategy makes it possible to guarantee a minimum amount of bandwidth for certain traffic types, while at the same time making the bandwidth that is left unused available to other traffic types.

c. **Weighted Fair Queuing (WFQ).** WFQ is a packet scheduling technique allowing guaranteed bandwidth services. The purpose of WFQ is to let several sessions share the same link by assigning weights' to each of the queues.

d. **Class-Based Weighted Fair Queuing (CBWFQ).** CBWFQ allows traffic to be weighted based on criteria, such as access control lists, input interface names, protocols, and QoS labels.

A3.3.3.2 Policing

[REQUIRED: C2VGLAN (converged), VGLAN (converged) - CONDITIONAL: C2VGLAN (non-converged), VGLAN (non-converged)] Traffic Policing limits the input or output transmission rate of a class of traffic based on user-defined criteria and marks packets by setting the IP Precedence value, the QoS group, or the DSCP value. **For converged LANs, the routers shall support at least one of the following policing mechanisms:**

a. **DiffServ Per-Hop Behavior (PHB):** a description of the externally observable forwarding treatment applied at a differentiated services-compliant node to a behavior aggregate based on the DSCP and as explained in RFCs 2474, 2475, and 3260.

If DiffServ is used, routers shall support the following:

1) **Expedited Forwarding (EF).** The EF PHB is defined in RFC 3246 as a forwarding treatment for a particular diffserv aggregate where the departure rate of the aggregate's packets from any diffserv node must equal or exceed a configurable rate. The EF traffic should receive this rate independent of the intensity of any other traffic attempting to transit the node. If the EF PHB is implemented by a mechanism that allows unlimited preemption of other traffic (e.g., a priority queue), the implementation shall include some means to limit the damage EF traffic could inflict on other traffic (e.g., a token bucket rate limiter). Traffic that exceeds this limit shall be discarded.

2) **Assured Forwarding (AF)**. The AF PHB group, as defined in RFC 2597, provides delivery of IP packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. A congested DS node tries to protect packets with a lower drop precedence value from being lost by preferably discarding packets with a higher drop precedence value. A DS node must allocate forwarding resources (buffer space and bandwidth) to AF classes so that, under reasonable operating conditions and traffic loads, packets of an AF class x do not have higher probability of timely forwarding than packets of an AF class y if x < y.

3) **Default Best Effort (BE)**. This is the common, best-effort forwarding behavior available in existing routers. When no other agreements are in place, it is assumed that packets belong to this aggregate. Such packets may be sent into a network without adhering to any particular rules and the network will deliver as many of these packets as possible and as soon as possible, subject to other resource policy constraints. **This forwarding behavior shall not be used for VoIP.**b.

Generic Traffic Shaping (GTS). GTS shapes traffic by reducing outbound traffic flow to avoid congestion by constraining traffic to a particular bit rate using the token bucket mechanism. GTS applies on a per-interface basis and can use access lists to select the traffic to shape. Traffic adhering to a particular profile can be shaped to meet downstream requirements, eliminating bottlenecks in topologies with data rate mismatches.

c. **Class-Based Shaping (CBS).** CBS is a modification to GTS in that CBS shapes on a traffic class basis, specifies average rate or peak rate traffic shaping, and uses CBWFQ.

A3.3.3.3 Virtual LANs (VLANs)

[REQUIRED: C2VGLAN (converged), VGLAN (converged) - CONDITIONAL: C2VGLAN (non-converged), VGLAN (non-converged)] There are three key standards for layer 2 switching and VLAN processing. These standards are governed by the IEEE and are 802.1D, 802.1p, and 802.1Q:

a. The 802.1D standard defines the notion of a bridge and how the spanning tree protocol works to define bridges and bridge membership.

b. 802.1p adds the notion of queue prioritization that defines up to eight prioritized traffic classes. This enables traffic to be tagged for faster or prioritized delivery.

c. Finally, 802.1Q defines the VLAN tag and associated processing. This specification also functionally specifies VLAN Registration among VLAN-aware Ethernet switches (Generic VLAN Registration Protocol, or GVRP). 802.1Q also talks about multicast registration (GMRP).

In general, there are three basic methods for determining and controlling how a packet gets assigned to a VLAN.

a. Port-based VLANs. Port-based VLANs are the simplest form of virtual LAN, but provide the largest degree of control and security. In this method, the administrator assigns each port of an Ethernet switch to a VLAN. For example, ports 1-3 might be assigned to VLAN 1, ports 4-6 to VLAN 2 and ports 7-9 to VLAN 3. The Ethernet switch determines the VLAN membership of each packet by noting the port on which it arrives; port assignments are static and can only be changed by the network administrator.

b. MAC address-based VLANs. The VLAN membership of a packet in this case is determined by its source or destination MAC address. Each Ethernet switch maintains a table of MAC addresses and their corresponding VLAN memberships. In order for a machine to gain access to the VLAN, it must have a MAC address that is recognized by the Ethernet switch.

c. Layer 3 (or protocol)-based VLANs. With this method, the VLAN membership of a packet is based on protocols and Layer 3 addresses.

Another important distinction between VLAN implementations is the method used to indicate membership when a packet travels between Ethernet switches. Two methods exist - implicit and explicit.

a. Implicit - VLAN membership is indicated by the MAC address. In this case, all Ethernet switches that support a particular VLAN shall share a table of member MAC addresses.

b. Explicit - A tag is added to the packet to indicate VLAN membership. The IEEE 802.1Q VLAN specification uses this method.

To summarize, when a packet enters its local Ethernet switch, the determination of its VLAN membership can be port-based, MAC-based or protocol-based. When the packet travels to other Ethernet switches, the determination of VLAN membership for that packet can be either implicit (using the MAC address) or explicit (using a tag that was added by the first Ethernet switch). Port-based and protocol-based VLANs use explicit tagging as their preferred indication method. MAC-based VLANs are almost always implicit.

For converged LANs, Ethernet switches shall support either Implicit or Explicit VLAN membership for:

a. Port-based VLANs

b. MAC address-based VLANs

c. Layer 3 (or protocol)-based VLANs

This requirement does not preclude softphones that may share the same virtual connection from the personal computer to the access switch where the traffic will be separated into the appropriate VLAN.

Network Management and Voice traffic (signaling & media) shall be placed in a separate VLAN from data and video traffic. CoS and QoS measures shall be applied to the network management and the voice VLAN to guarantee bandwidth.

A3.3.4 LAN Design

[REQUIRED: C2VGLAN, VGLAN] LANs can be designed to be ”shared” or ”switched”. Typically, shared topologies share bandwidth (10 Mbps or 100 Mbps) amongst a fixed number of users while switched LAN topologies dedicate bandwidth (10 Mbps or 100 Mbps) to each subscriber. Switched LANs can be half duplex (one-way communications) or full duplex (two-way simultaneous communications). **For VoIP solutions, C2VGLAN networks shall be designed to support a full duplex switched topology.**

All C2VGLAN networks shall be designed not to exceed the IEEE recommended distances for Ethernet cabling provided in Table 1 below. Ethernet switching platforms used in the

LAN shall conform to the IEEE standards listed in Table 2. For VoIP implementations, the following paragraphs detail the network design requirements that shall be met.

Table 1. IEEE 802.3 Distance Limitations

	10Base-T Ethernet	100Base-T Fast Ethernet	1000Base-T Gigabit Ethernet
Cat 5 & 6 UTP, Cat 5e	330 ft 100 m	330 ft 100 m	330 ft 100 m
Multi-mode Fiber	6600 ft 2 km	6600 ft 2 km	1830 ft 550 m
Single-mode Fiber	15 mi 25 km	12 mi 20 km	3 mi 5 km
Note: All distances are for full duplex communications.			
Legend: Cat - Category ft - Feet km - Kilometers		m - Meters mi - Miles UTP - Unshielded Twisted Pair	

Table 2. IEEE Conformance for LAN Switches used in Converged Networks

Switching Platforms IEEE Conformance	
Standard	**Description**
802.1d	Bridging
802.1p/Q	VLAN tagging
802.1s	Per-VLAN Group Spanning Tree Protocol
802.1v	VLAN Classification by Protocol and Port
802.1w	Rapid Reconfiguration of Spanning Tree
802.1x	Port Based Network Access Control
802.3ad	Link Aggregation Protocol
Legend: IEEE - Institute of Electrical and Electronic Engineers Inc LAN - Local Area Network	VLAN - Virtual LAN

A3.3.4.1 Reliability

[REQUIRED: C2VGLAN - CONDITIONAL: VGLAN] The following paragraphs outline the reliability requirements for the C2VGLAN. **The C2VGLAN shall have a hardware availability of .99999 (non-availability of no more than 5 minutes per year (mins/yr)). The vendor shall provide a reliability model for the system showing all calculations and showing how the overall availability will be met. The C2VGLAN shall have no single point of failure that can cause an outage of more than 64 telephony subscribers. In order to meet**

the availability requirements, all switching/routing platforms that offer service to more than 64 telephony subscribers shall have a modular chassis that provides at a minimum:

a. **Dual power supplies**. The platform shall provide a minimum of two power supplies each with the power capacity to support the entire chassis. Loss of a single power supply shall not cause any loss of ongoing functions within the chassis.

b. **Dual processors (control supervisors)**. The chassis shall support dual active processors. Failure of any one processor shall not cause loss of any ongoing functions within the chassis (e.g. no loss of active calls).

c. **Termination Sparing**. The chassis shall support a (N + 1) sparing capability for available 10/100 Base-T modules used to terminate to an IP subscriber.

d. **Redundancy protocol**. Routing equipment shall support a protocol that allows for dynamic rerouting of IP packets so that no single point of failure exists in the C2VGLAN.

e. **No Single Failure Point**. No single point shall exist in the LAN that would cause loss of voice service to more than 64 IP telephony instruments.

f. **Switch Fabric or Backplane Redundancy**. Switching platforms within the C2VGLAN shall support a redundant (1 + 1) switching fabric or backplane. The second fabric's backplane shall be in active standby such that failure of the first shall not cause loss of ongoing events within the switch.

The components that comprise the C2VGLAN systems for C2 users shall meet the appropriate GSCR switch type backup power requirements (e.g., 8 hours for MFS/SMEO/EO) for all devices including the phones. For a PBX1, the backup power requirement is 2 hours.

In the event of a component failure in the network, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the path through the network shall be restored within 2 seconds. All devices used to build redundancy shall be capable of handling the entire call processing load in the event that its counterpart device fails.

A3.3.4.1.1 <u>Maximum Downtime</u>

[REQUIRED: TS, EOS, MFS, SMEO - CONDITIONAL: PBX1, PBX2] Individual IP telephone terminations shall meet the following maximum downtime requirements:

a. IP (10/100 Ethernet) network links - 35 mins/yr

b. IP subscriber - 12 mins/yr

[REQUIRED: PBX1 – CONDTIONAL: PBX2] PBXs shall meet the following maximum downtime requirements:

a. IP (10/100 Ethernet) network links - 80 mins/yr

b. IP subscriber - 120 mins/yr

A3.3.4.2 Management

A3.3.4.2.1 Interface

[REQUIRED: C2VGLAN - CONDITIONAL: VGLAN] For management of the LAN, there are two methods to physically interface to the LAN devices; in-band and out-of-band. The in-band method includes one approach, which is via an Ethernet port. The out-of-band method includes three different approaches, which are via an Ethernet port, local port, or an internal modem. **Each device in a LAN shall support at least one of the following methods:**

a. **In-band**. Network management system connects to the network device using the same communication channels used for user traffic.

1) **Ethernet Port. Network management system connects to the network device using the same Ethernet network as the user traffic.**

b. **Out-of-band**. Network management system connects to the network device using a physically separated network from the network used for user traffic. This requires an additional network infrastructure to support management traffic.

1) **Ethernet Port. Network management system connects to the network device using a different Ethernet network than used for user traffic.**

2) **Local port. Network management system connects to the network device via a local port (i.e., RS-232 port) on the device using a computer, terminal or modem.**

3) **Modem. Network managers connect to the network device remotely using an integrated modem interface on the device. Communications are usually over the Public Switched Telephone Network (PSTN) and operators may dial in from remote locations.**

[REQUIRED: C2VGLAN - CONDITIONAL: VGLAN] Simple Network Management Protocol (SNMP) shall be used as a minimum for interfacing between the LAN devices and the network management system. SNMP guidance is contained in the SNMPv3 Compliance Requirements for DISA, 1 July 2003, which require that SNMPv1, SNMPv2c, and SNMPv3 are supported and that at least the User-based Security Model (Request for Comment (RFC) 3414) and the Community-based Security Model (RFC 2576) are implemented. The document also contains a list of the SNMP RFCs that are required by network management systems. It is an objective requirement that only SNMPv3 is implemented. In addition, both RMON2 and MIB II shall be supported for SNMP implementations.

In addition, if other methods are used for interfacing between LAN devices and the network management system they shall be implemented in a secure manner such as with the following methods:

a. **Secure Shell 2 (SSH2). The SSH2 protocol shall be used instead of Telnet due to its increased security as described in Internet Draft "draft-ietf-secsh-transport-17.txt – SSH Transport Layer Protocol."**

b. **HyperText Transfer Protocol, Secure (HTTPS). HTTPS shall be used instead of HTTP due to its increased security as described in RFC 2660 "Secure HyperText Transfer Protocol."**

A3.3.4.2.2 Measurements

[REQUIRED: C2VGLAN - CONDITIONAL: VGLAN] LAN devices shall be capable of measuring and reporting the following measurements:

a. **Performance. The VoIP Network Management System shall collect statistics and monitor bandwidth utilization, delay, jitter, and packet loss.**

b. **Fault. The VoIP LAN transport elements (e.g., routers, Ethernet switches, etc.) shall provide** status changes to the network management system by an automated capability in near real time (less than one minute) 99.95% (Objective) and 99.5% (Threshold) of the time. **The automated status change requirements are satisfied by sending SNMP or ASCII messages from the VoIP LAN components to the VoIP network management system.**

c. **Configuration. The VoIP network management system shall have the ability to perform remote configuration/reconfiguration of objects that have existing DoD Joint Technical Architecture (JTA) management capabilities or permit configuration/ reconfiguration via one of the protocols specified in section A3.3.4.2.1.**

d. **For security and control purposes, VoIP LAN devices shall only be activated by a central control entity (e.g., help desk or service office). "Plug and Play" shall not be enabled. All DOD security policies and guidelines for IP networks shall be adhered to when designing the NM capabilities of the LAN.**

A3.3.4.3 Security

[REQUIRED: C2VGLAN, VGLAN] The IP equipment that comprises the C2VGLAN and/or the VGLAN shall provide the features and functionality needed to implement the requirements of the Network Infrastructure and the VoIP STIG. Where there is a direct conflict of requirements (e.g., stateful packet inspection firewall requirement versus application firewall requirement) between the two STIGs, the VoIP STIG requirements shall take precedence. Where no conflicts exist in requirements, the features and functionality needed to implement the requirements of both STIGs apply simultaneously.

A3.3.4.4 Traffic Engineering (TE)

A3.3.4.4.1 Bandwidth

[REQUIRED: C2VGLAN, VGLAN] Bandwidth required per subscriber is 178.4 kbps (89.2 kbps each direction) for each IP call. This is based on G.711with IP overhead (87.2 kbps) with VoIP signaling (2 kbps) included. Bandwidth available for Ethernet full duplex LANs is 20 Mbps (10 Mbps upstream and 10 Mbps downstream) and 200 Mbps (100 Mbps upstream and 100 Mbps downstream) for 10Base-T and 100Base-T, respectively. (For the purposes of this document, bandwidth is defined in the sense used in TDM telephony systems, i.e., the bandwidth of a T1 trunk is 1.544 Mbps for each direction, for a total full duplex bandwidth of 3.088 Mbps.) In order to provide non-blocking bandwidth for trunk traffic, 4.185 Megabits per second (Mbps) shall be reserved in the LAN for each T1 trunk between the Gateway and DSN. This bandwidth requirement is based on 24 simultaneous two-way non-compressed G.711 conversations (24x 174.4 kbps). Bandwidth shall be guaranteed through the use of CoS/QoS as described in this appendix. (Based on overhead bits included in the bps calculations, vendor implementations may use different bps calculations and hence arrive at slightly different bps numbers. This is acceptable to the government, but does not negate the number of IP telephone subscribers that are allowed per 10, 100, 1000 Mbps link as specified in Sections A3.3.4.4.2 through A3.3.4.5.1.1).

A3.3.4.4.2 TE Calculations

[REQUIRED: C2VGLAN, VGLAN] LAN architectures proposed for VoIP systems shall be designed based on the following traffic engineering parameters:

a. Bandwidth for 64 subscribers is 5.71 Mbps (11.42 Mbps for two-way conversation); 64 subscribers can be serviced via a 10 Mbps full duplex link.

b. The physical interface between the LAN and Local Call controller/Gateway shall be a minimum of 100 Mbps Ethernet (full duplex).

c. Maximum number of IP telephony subscribers per 100 Mbps full duplex link to the IP Gateway or TDM switch is 1024. For interface cards in the circuit switch or in the VoIP call control device that cannot support 1024 simultaneous IP subscribers, the number of subscribers is limited to the maximum number of simultaneous calls the interface card can support.

d. Access links (between IP phone/Ethernet switch) shall be switched 10 Mbps or 100 Mbps Ethernet.

A3.3.4.4.3 Non-Converged LAN TE

[REQUIRED: C2VGLAN - CONDITIONAL: VGLAN] For non-converged LANs, each switching/routing component's network links shall be engineered as follows:

a. **10 Mbps single link.** Up to 64 IP telephony subscribers may be supported per 10 Mbps single link for the C2VGLAN. The VGLAN may support up to 100 IP telephony subscribers per 10 Mbps link because it does not have to support single point of failure requirements of section A3.3.4.1 above (i.e., 64 IP subscribers).

b. **10 Mbps link pair.** Up to 100 IP telephony subscribers may be supported per 10 Mbps link for the C2VGLAN if reliability requirements are met. A 10 Mbps link pair is not required for the VGLAN.

c. **100 Mbps/1 Gbps single link.** Up to 64 IP telephony subscribers may be supported per link for the C2VGLAN. For the VGLAN, up to 1024 IP telephony subscribers can be supported per link.

d. **100 Mbps/1 Gbps Link pair**. Up to 1024 IP telephony subscribers can be supported per link pair on one device if reliability requirements are met.

A3.3.4.4.4 Converged LAN TE

[REQUIRED: C2VGLAN - CONDITIONAL: VGLAN] For converged LANs, switching/routing component's network links shall be engineered as follows:

a. **100 Mbps/1 Gbps single link.** Up to 64 IP telephony subscribers may be supported per link for the C2VGLAN. For the VGLAN, up to 1024 IP telephony subscribers can be supported per link.

b. **100 Mbps link pair**. Up to 256 IP telephony subscribers may be supported per link pair for the C2VGLAN. Up to 1024 IP telephony subscribers may be support per link pair for the VGLAN.

c. **1 Gbps link pair.** Up to 1024 IP telephony subscribers may be supported per link pair for the C2VGLAN and VGLAN.

A3.3.4.5 LAN Architectures

A3.3.4.5.1 C2VGLAN

C2VGLANs will be designed to ensure that traffic engineering and redundancy requirements specified in the GSCR are met. C2 LANs may be designed to use any combination of the following layers:

a. Access or edge layer. The access or edge layer is the point at which local end users are allowed into the network. This layer may also use access lists or filters to further optimize the needs of a particular set of users.

b. Distribution or building layer. The distribution or building layer of the network is the demarcation point between the access and core layers and helps to define and differentiate the core. The purpose of this layer is to provide boundary definition and is the place at which packet manipulation can take place.

c. Core layer. The core layer is a high-speed switching backbone and is designed to switch packets as fast as possible.

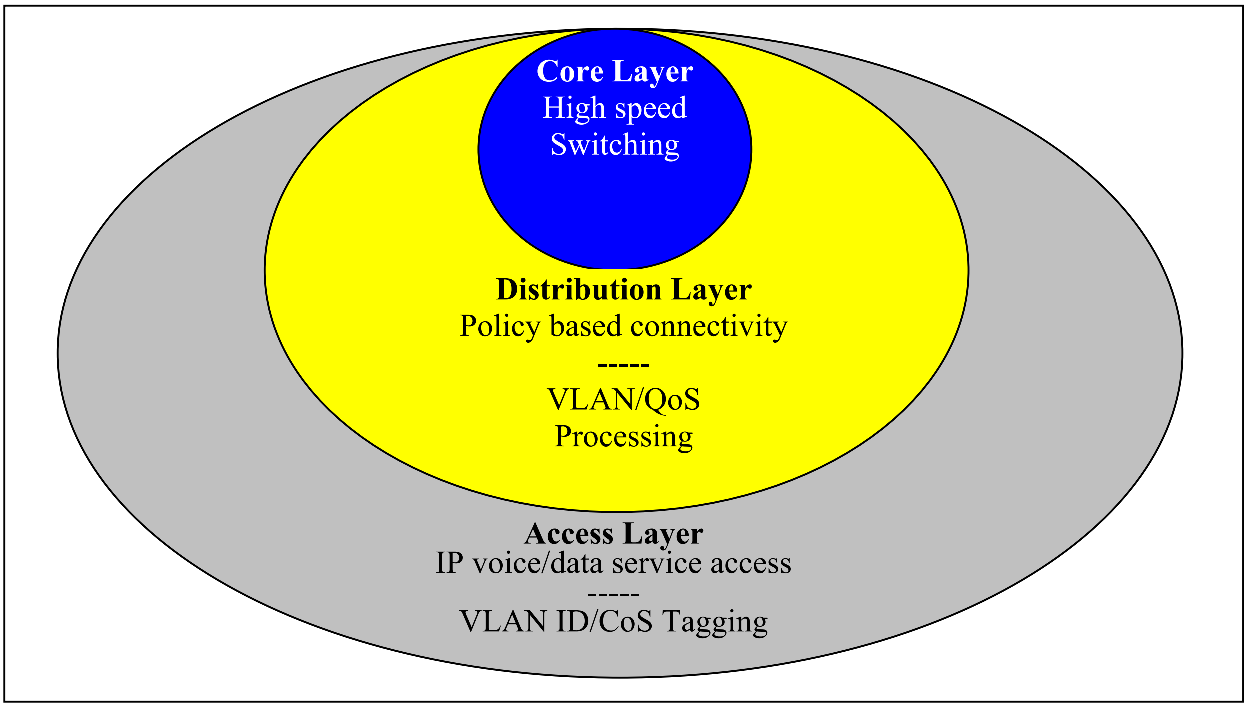


Figure 5. LAN Layers

A3.3.4.5.1.1 <u>Access Layer</u>

For the C2VGLAN, access from the IP subscriber shall be provided by Ethernet switches. There are two methods that an IP subscriber can access voice services: dedicated Ethernet port or shared Ethernet port. Dedicated access method provides separate access ports for Voice and other traffic type. Shared access method allows a single access port to provide for all traffic types. **C2VGLANs may use either method (see figure 6) but shall use VLANs to separate voice from other traffic.** Access switches used in the C2VGLAN may range in size from less than 64 voice IP subscriber ports to 1024 voice IP subscriber ports. For access devices that provide IP voice services to more than 64 IP telephony users the switch shall meet the reliability requirements described in section A.3.3.4.1 of this appendix. For data PC ports, the number of ports for dedicated access is not specified.

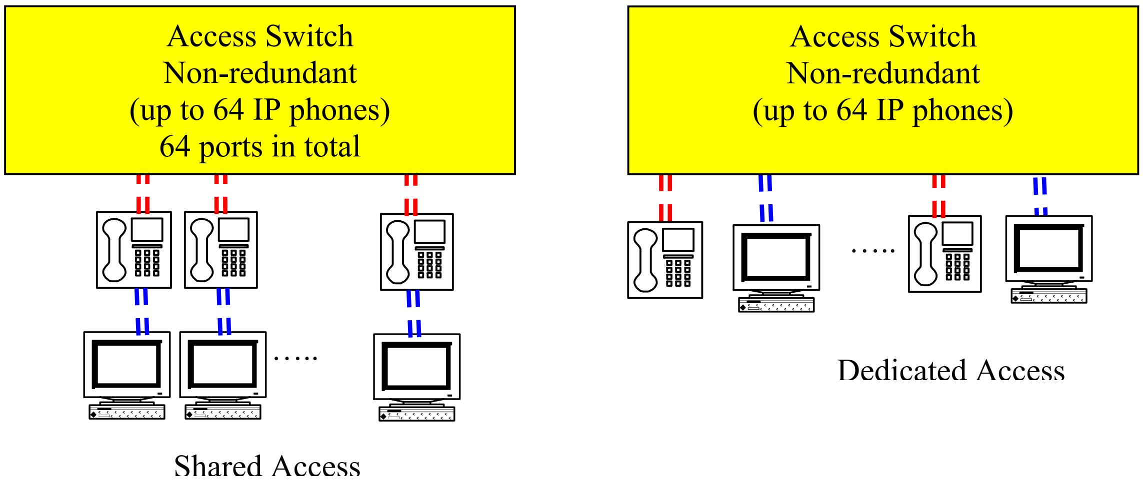


Figure 6. Access Methods for Converged C2VGLAN

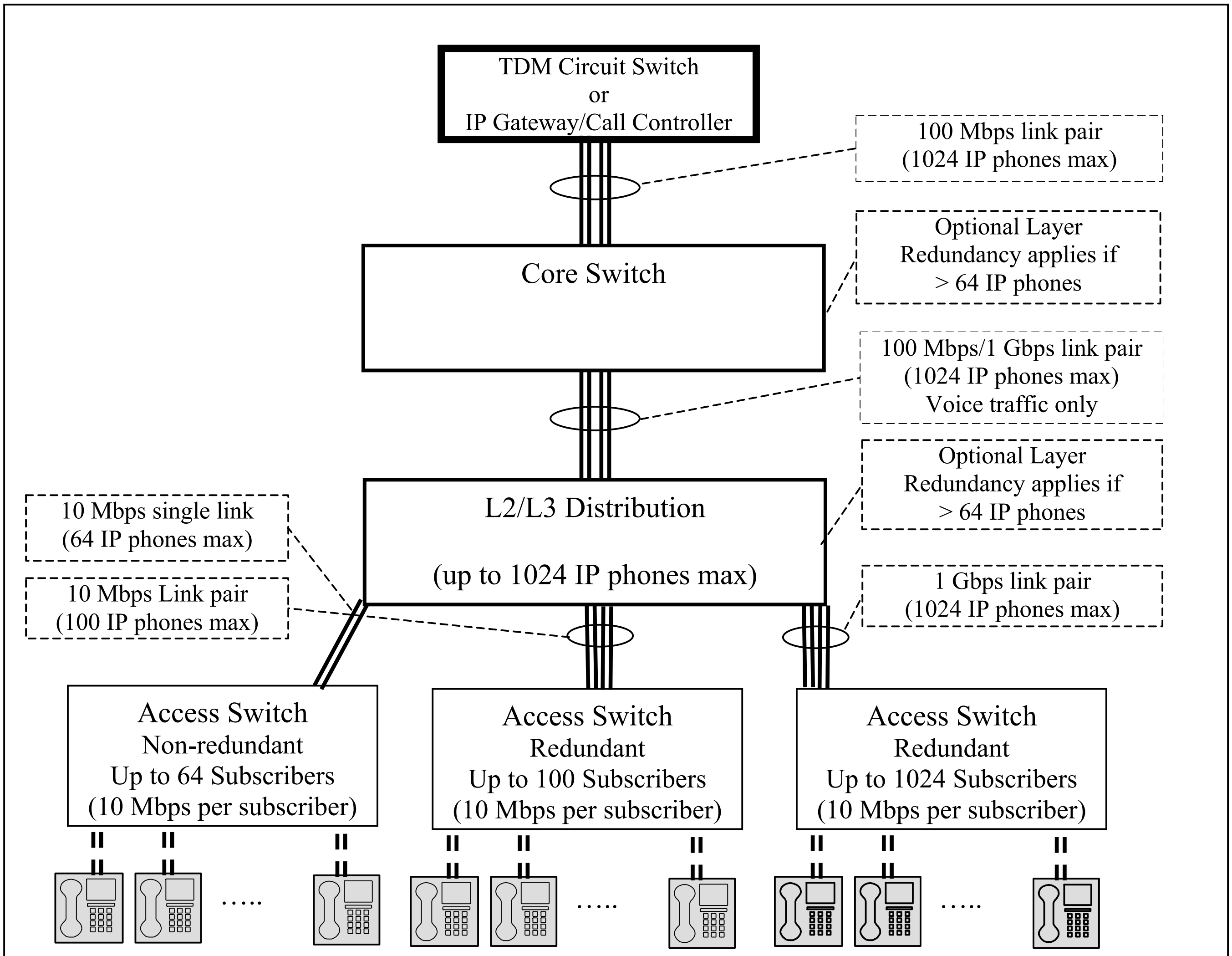
A3.3.4.5.1.1. Distribution & Core Layers

If a distribution layer or core layer is implemented, networks links between an access device and the devices shall be:

a. Non-converged C2 VGLAN. Minimum one 100 Mbps link pair for every 1024 IP telephony subscribers.

b. Converged C2 VGLAN. Minimum one 100 Mbps link pair for every 256 IP telephony subscribers or minimum one 1 Gbps link pair for every 1024 subscribers (e.g., 512 IP telephones require at a minimum two 100 Mbps link pairs, 1024 IP phones require either four 100 Mbps link pairs or one 1 Gbps link pairs).

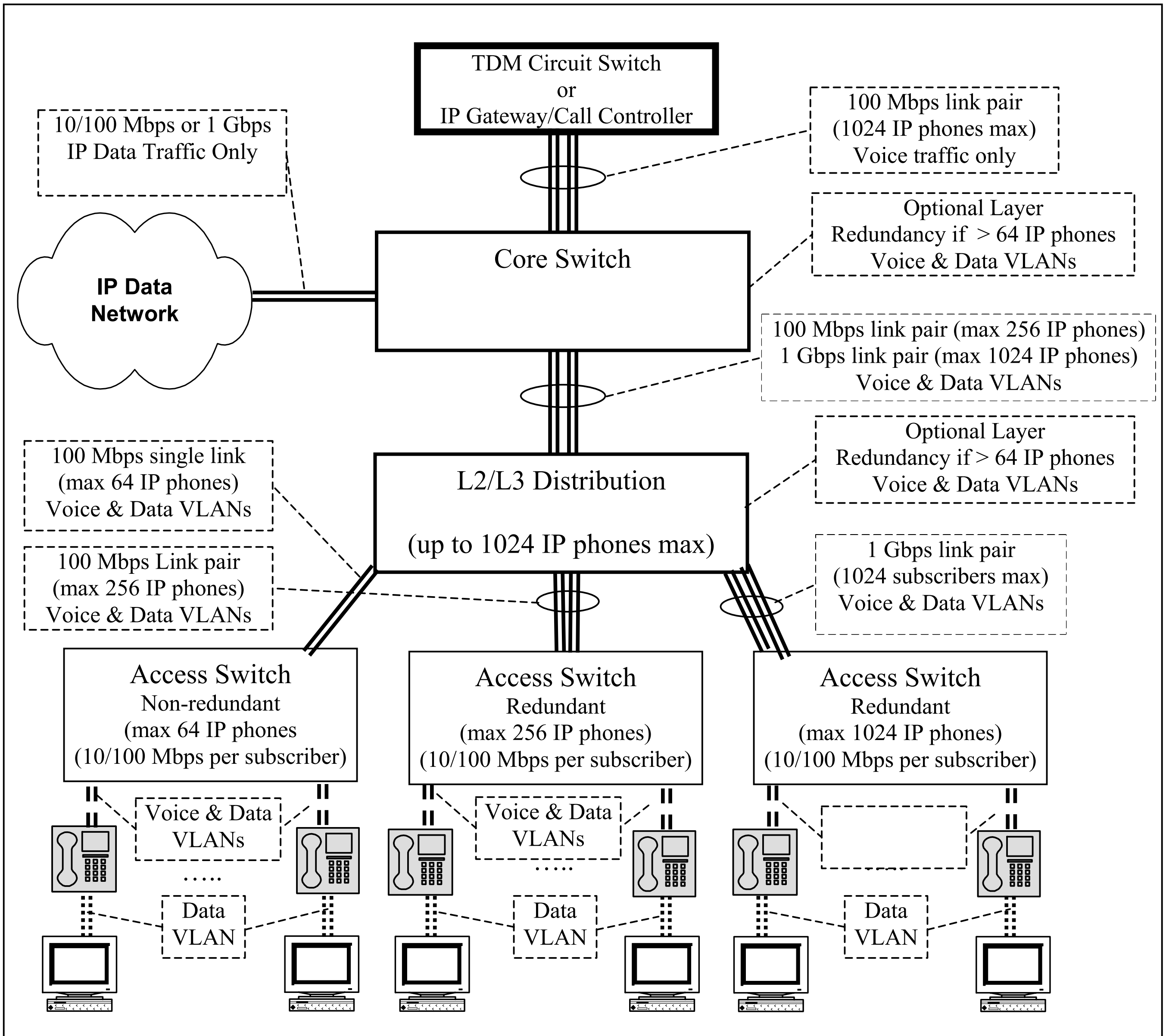
Figures 7, 8, and 9 depict the pictorial architectures that could be implemented for the C2VGLAN.



Notes:
1. All Links are full duplex.

C2	- Command & Control	LAN	- Local Area Network
IP	- Internet Protocol	Mbps	- Megabits per second
L2	- Open Systems Interconnect Layer 2 (Switching)	TDM	- Time Division Multiplexing
L3	- Open Systems Interconnect Layer 3 (Routing)		

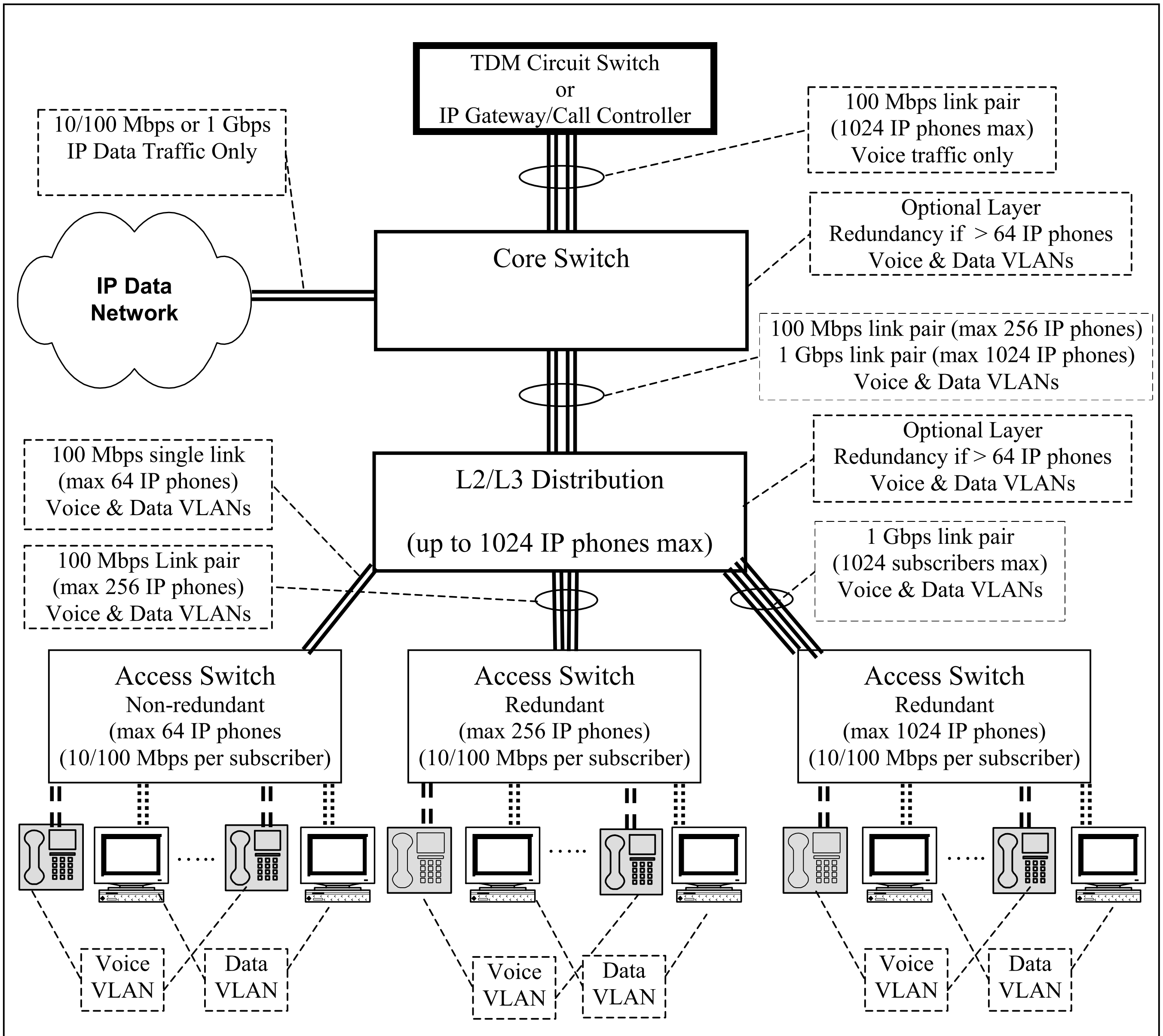
Figure 7. C2VGLAN (non-converged) Architecture



Notes:
1. All links are Full duplex.

C2	- Command & Control	LAN	- Local Area Network
IP	- Internet Protocol	Mbps	- Megabits per second
L2	- Open Systems Interconnect Layer 2 (Switching)	TDM	- Time Division Multiplexing
L3	- Open Systems Interconnect Layer 3 (Routing)	VLAN	- Virtual LAN

Figure 8. C2VGLAN (converged) Architecture with Shared Access



Notes:
1. All links are Full duplex.

C2	- Command & Control	LAN	- Local Area Network
IP	- Internet Protocol	Mbps	- Megabits per second
L2	- Open Systems Interconnect Layer 2 (Switching)	TDM	- Time Division Multiplexing
L3	- Open Systems Interconnect Layer 3 (Routing)	VLAN	- Virtual LAN

Figure 9. C2VGLAN (converged) Architecture with Dedicated Access

A3.3.4.5.2 VGLAN

[REQUIRED: PBX2] Though not required to provide C2 services, VGLANs are still required to provide voices services in accordance with CJCSI 6215.01B. VGLANs used to provide PBX2 voice services shall be designed in a manner consistent with PBX2 design practices. VGLANs will be designed in a manner similar to those presented for the C2 VGLAN with the exception that redundancy and single point of failure considerations need not be included.

A3.4 Requirements Summary

Table 3 provides a summary of the LAN requirements provided in the paragraphs above. Tables 4 and 5 provide the requirements for routers (Layer 3) or switches (Layer 2) used within the LAN.

Table 3. Overall LAN Requirements Summary

LAN Requirements (C2VGLAN & VGLAN)		
Description	**Requirement**	**Reference**
Voice Quality	MOS 4.0 or better	CJCSI 621501.B
Codec	G.711 (64 kbps)	GSCR
MLPP	MLPP interaction	GSCR
Delay	< 60 msec one-way for system < 5 msec one-way for the LAN	DISAHQ
Network Jitter	< 5 msec	DISAHQ
Network Packet Loss	< 0.05%	DISAHQ
Bandwidth (one way)	89.2 kbps(NOMINAL)	GSCR/DISAHQ
Availability (SMEO-MFS) Availability (PBX 1)	99.999% C2VGLAN GSCR Reliability/Failure - 35 mins/yr - 12 mins/yr 99.999% C2VGLAN 99.997% PBX 1 availability - 80 mins/yr - 120 mins/yr	 GR-512-CORE/GR-474-CORE - IP network link downtime - IP Subscriber downtime GSCR - IP network link downtime - IP Subscriber downtime
Battery backup/UPS	MFS, EO,& SMEO - 8 hrs PBX1 - 2 hrs if no alternate power source	GSCR

LAN Requirements (C2VGLAN & VGLAN)		
Description	**Requirement**	**Reference**
Legend: C2 - Command and Control Cat - Category DVGR - DOD Voice Gateway Requirements EO - End Office GSCR - Generic Switching Center Requirements Hrs - Hours IEEE - Institute of Electrical and Electronic Engineers Inc. Kbps - Kilobits per second LAN - Local Area Network MLPP - Multi-level Precedence and Preemption MFS - Multifunction Switch Msec - Millisecond MOS - Mean Opinion Score SMEO - Small End Office UPS - Uninterruptible Power Supply		

Table 4. LAN Platform Requirements

LAN Routing (C2VGLAN & VGLAN)	
Description	**Requirement**
Chassis	Modular (see Note 1)
Power Supplies	Minimum dual configuration (see Note 1)
Control Supervisor modules	Minimum dual configuration (see Note 1)
NM	Ethernet, serial port or integrated modem
CoS (any one of)	IEEE 802.1 p/Q DSCP- RFC 2474 802.1p to DSCP mapping IP TOS - RFCs 1060/1349/1583/1700
QoS (any one of)	Queuing - CQ - WFQ - CBWFQ
	Policing - DiffServ PHB - GTS - CBS
Notes: 1. Required for C2VGLAN; conditional for VGLAN)	

LAN Routing (C2VGLAN & VGLAN)	
Description	**Requirement**
Legend: AF - Assured Forwarding BE - Best Effort CBWFQ - Class-Based Weighted Fair Queuing CBS - Class-Based Shaping CoS - Class of Service CQ - Custom Queuing DiffServ - Differentiated Services DSCP - DiffServ Code Point EF - Expedited Forwarding GTS - Generic Traffic Shaping IEEE - Institute of Electrical and Electronic Engineers Inc.	 IP - Internet Protocol NM - Network Management PHB - Per-Hop Behavior PBR - Policy- Based Routing PQ - Priority Queuing QoS - Quality of Service RFC - Request for Comment RSVP - Resource Reservation Protocol TOS - Type of Service WFQ - Weighted Fair Queuing

Table 5. LAN Ethernet Switching Platform Requirements

LAN Ethernet (C2VGLAN & VGLAN)	
Description	**Requirement**
Chassis	Modular (see Notes 1)
Power Supplies	Minimum dual configuration (see Note 1)
Control Supervisor modules	Minimum dual configuration (see Note 1)
Switch Fabric	Redundant (1+1) (see Note 1)
(N + 1) 10/100 Mbps modules	IEEE 802.3 (see Note 1)
IEEE Conformance 802.1d	Bridging
802.1p/Q	VLAN tagging
802.1s	Per-VLAN Group Spanning Tree Protocol
802.1w	Rapid Spanning Tree Protocol
802.1x	Port Based Access Control
802.3ad	Link Aggregation Protocol
CoS	Any one of: - IEEE 802.1 p/Q - DSCP- RFC 2474 - IP TOS - RFCs 1060/1349/1583/1700
QoS	Queuing (any one of) - CQ - WFQ - CBWFQ
	Policing (any one of) - DiffServ PHB - GTS - CBS
	VLANs - Port-based VLANs - MAC address-based VLANs - Layer 3 (or protocol)-based VLANs - Implicit VLAN membership - Explicit VLAN membership
Notes: 1. Required for C2VGLAN devices with more than 64 IP telephony subscribers; conditional for VGLAN.	

LAN Ethernet (C2VGLAN & VGLAN)	
Description	**Requirement**
Legend:	
AF - Assured Forwarding	IP - Internet Protocol
BE - Best Effort	NM - Network Management
CBWFQ- Class-Based Weighted Fair Queuing	PHB - Per-Hop Behavior
CBS - Class-Based Shaping	PBR - Policy- Based Routing
CoS - Class of Service	PQ - Priority Queuing
CQ - Custom Queuing	QoS - Quality of Service
DiffServ- Differentiated Services	RFC - Request for Comment
DSCP - DiffServ Code Point	RSVP - Resource Reservation Protocol
EF - Expedited Forwarding	TOS - Type of Service
GTS - Generic Traffic Shaping	WFQ - Weighted Fair Queuing
IEEE - Institute of Electrical and Electronic Engineers Inc.	

Enclosure A
DSN Switch Interface Requirements

Trunk Type	TS	MFS	EO	SMEO	PBX1
T1 SS7 (T1 619a)	R	R	R		
E1 SS7 (ITU-T Q.955.3, Q.735.3 (R=EUROPE ONLY)	R	R	R		
T1 CAS MF R1	R	R	R		
T1 CAS DTMF	R	R	R	R	
T1 CAS DP	R	R	R	R	
E1 CAS MF R1 (R=EUROPE ONLY)	R	R	R	R	
E1 CAS DTMF (R=EUROPE ONLY)	R	R	R	R	
E1 CAS DP (R=EUROPE ONLY)	R	R	R	R	
T1 ISDN PRI (ANSI T1.619a)	R	R	R	R	R
ISDN PRI Subscriber NI-2	R	R	R	R	R
E1 ISDN PRI (ITU-T Q.955.3, Q.735.3) (R=EUROPE ONLY)	R	R	R		
Line Type	**TS**	**MFS**	**EO**	**SMEO**	**PBX1**
2-wire analog Lines		R	R	R	R
ISDN BRI Subscriber NI-1		R	R	R	R
ISDN BRI Subscriber NI-2		R	R	R	R
ISDN-BRI ANSI T1-619a		R	R	R	R

Enclosure B
DSN Switch Type Interface/Feature Requirements

Multi-Function Switch				
Switch	**Trunk**	**Line**	**NM**	**Attendant**
	Interface			
	- T1 SS7 (T1.619a) - E1 SS7 (Q.955.3/Q.735.3) (Europe only) - T1 CAS MF R1 - T1 CAS DTMF - T1 CAS DP - E1 CAS MF R1 (Europe only) - E1 CAS DTMF (Europe only) - E1 CAS DP (Europe only) - T1 ISDN PRI T1.619a - T1 ISDN PRI NI-2 - E1 ISDN PRI (Q.955.3/Q.735.3) (Europe only)	- 2W Analog - ISDN BRI NI-1/NI-2 - ISDN BRI T1.619a	- Ethernet TCP/IP - Serial RS-232 - X.25 or BX.25	
Feature/Capability				
- Code Restriction & Diversion (2.1.4) - Public Safety Features (2.4) - Local office Test lines (2.5.1) - Outside Plant Test lines (2.5.2) - Manual Testing (2.5.4) - Trunk Group -make busy (2.5.5) - Trunk Group- Make Idle (2.5.6) - Carrier Group Alarms (2.5.7)	- ISDN NI 1/2 PRI (2.3.4) - CAS MLPP (3.4.1) - PRI MLPP (3.4.2) - CCS7 MLPP (3.4.3) - ISDN MLPP PRI (3.7) - MLPP CCS7 (3.9) - CAS to CCS trunk interworking (3.10) - DSN IST Call Processing (4.4) - DSN switch outpulsing (4.5.2) - Trunk Supervisory Signaling (5.3) - Control Signaling (5.4) - CCS7 (5.6)	- DN Identification (2.1.1) - PBX line (2.3.1) - Direct inward dial (2.3.2) - ISDN NI 1/2 BRI (2.3.3) - Analog Line (2.3.5) - Analog Line MLPP (3.5) - ISDN MLPP BRI (3.6) - 2W User Access (4.3.3)	- NM Manual controls (3.13) - Data Collection (3.14) - NTMOS (9.1) - Common Data Requirements (9.2.1) - Cct Switched Net. Measurements (9.2.2) - CCS NM (9.2.3) - ISDN Measurements (9.2.4) - Traffic Capacity (9.2.5) - Configuration Mgmt (9.3)	- Precedence & Preemption (2.2.1) - Call display (2.2.2) - Class of service override (2.2.3) - Busy override/verification (2.2.4) - Night Service (2.2.5) - Auto recall of attendant (2.2.6) - Calls in queue (2.2.7) - Release to Pivot (2.2.8)

Multi-Function Switch				
Switch	**Trunk**	**Line**	**NM**	**Attendant**
- Preset Conferencing (2.6) - Address Translation (2.7) - Nailed-up connections (2.8) - Assured Dial Tone (2.9) - DSN hotline service (2.12) - MLPP (3.1) - Preemption in the Network (3.2) - Precedence Call Diversion (3.3) - Preset Conferencing MLPP (3.8.7) - COI (3.8.9) - Call Treatments (4.1) - Primary & Alternate Routing (4.2) - WWNDP (4.5.1) - Standard DNs (4.5.3) - Std test numbers (4.5.4) - Base Services - Abbrev. No. (4.5.5) - Digit Reception (4.5.6) - Digit Registration Capacity (4.5.7) - Screening (4.5.8) - Network Power (5.1) - Alerting Signals and Tones (5.5) - DSN Transmission (6) - IDLC (7.5) - Tandem Switching (8) - ISDN Generic Requirements (10) - Timing Modes (11.1) - Synchronization performance	- ISDN DSS1 (5.7) - PCM-24 (7.1) - PCM-30 (7.2) (Europe only) - PCM-24/PCM-30 Interoperation (7.3)	- Analog Line termination (4.3.4) - Line Signaling (5.2)	- Fault Management (9.4) - AMA CDR (9.5.1) - Data Retention (9.5.2) - Auto Controls (9.6.1) - Overload Controls (9.6.2) - Manual Controls (9.6.3) - Treatment options (9.6.4) - Remote Access (9.7) - AMA (9.8)	

Multi-Function Switch				
Switch	**Trunk**	**Line**	**NM**	**Attendant**
monitoring criteria (11.2) - DS1 traffic interfaces (11.3) - DS0 Traffic interconnects (11.4) - Reliability (12) - Security (13)				
Notes: 1. Above features show title description and GSCR paragraph (in brackets).				

<table>
<tr><th colspan="5">End Office (EO) Switch</th></tr>
<tr><th>Switch</th><th>Trunk</th><th>Line</th><th>NM</th><th>Attendant</th></tr>
<tr><td rowspan="2"></td><th colspan="4">Interface</th></tr>
<tr><td>- T1 SS7 (T1.619a)
- E1 SS7 (Q.955.3/Q.735.3) (Europe only)
- T1 CAS MF R1
- T1 CAS DTMF
- T1 CAS DP
- E1 CAS MF R1 (Europe only)
- E1 CAS DTMF (Europe only)
- E1 CAS DP (Europe only)
- T1 ISDN PRI T1.619a
- T1 ISDN PRI NI-2
- E1 ISDN PRI (Q.955.3/Q.735.3) (Europe only)</td><td>- 2W Analog
- ISDN BRI NI-1/NI-2
- ISDN BRI T1.619a</td><td>- Ethernet TCP/IP
- Serial RS-232
- X.25 or BX.25</td><td></td></tr>
<tr><th colspan="5">Feature/Capability</th></tr>
<tr><td>- Code Restriction & Diversion (2.1.4)
- Public Safety Features (2.4)
- Local office Test lines (2.5.1)
- Outside Plant Test lines (2.5.2)
- Manual Testing (2.5.4)
- Trunk Group -make busy (2.5.5)
- Trunk Group- Make Idle (2.5.6)
- Carrier Group Alarms (2.5.7)
- Preset Conferencing (2.6)
- Address Translation (2.7)
- Nailed-up connections (2.8)</td><td>- ISDN NI 1/2 PRI (2.3.4)
- CAS MLPP (3.4.1)
- PRI MLPP (3.4.2)
- CCS7 MLPP (3.4.3)
- ISDN MLPP PRI (3.7)
- MLPP CCS7 (3.9)
- CAS to CCS trunk interworking (3.10)
- DSN IST Call Processing (4.4)
- DSN switch outpulsing (4.5.2)
- Trunk Supervisory Signaling (5.3)
- Control Signaling (5.4)
- CCS7 (5.6)
- ISDN DSS1 (5.7)
- PCM-24 (7.1)
- PCM-30 (7.2) (Europe only)</td><td>- DN Identification (2.1.1)
- PBX line (2.3.1)
- Direct inward dial (2.3.2)
- ISDN NI 1/2 BRI (2.3.3)
- Analog Line (2.3.5)
- Analog Line MLPP (3.5)
- ISDN MLPP BRI (3.6)
- 2W User Access (4.3.3)
- Analog Line termination (4.3.4)
- Line Signaling (5.2)</td><td>- NM Manual controls (3.13)
- Data Collection (3.14)
- NTMOS (9.1)
- Common Data Requirements (9.2.1)
- Cct Switched Net. Measurements (9.2.2)
- CCS NM (9.2.3)
- ISDN Measurements (9.2.4)
- Traffic Capacity (9.2.5)
- Configuration Mgmt (9.3)
- Fault Management (9.4)
- AMA CDR (9.5.1)</td><td>- Precedence & Preemption (2.2.1)
- Call display (2.2.2)
- Class of service override (2.2.3)
- Busy override/verification (2.2.4)
- Night Service (2.2.5)
- Auto recall of attendant (2.2.6)
- Calls in queue (2.2.7)
- Release to Pivot (2.2.8)</td></tr>
</table>

End Office (EO) Switch				
Switch	**Trunk**	**Line**	**NM**	**Attendant**
- Assured Dial Tone (2.9) - DSN hotline service (2.12) - MLPP (3.1) - Preemption in the Network (3.2) - Precedence Call Diversion (3.3) - COI (3.8.9) - Call Treatments (4.1) - Primary & Alternate Routing (4.2) - WWNDP (4.5.1) - Standard DNs (4.5.3) - Std test numbers (4.5.4) - Base Services - Abbrev. No. (4.5.5) - Digit Reception (4.5.6) - Digit Registration Capacity (4.5.7) - Screening (4.5.8) - Network Power (5.1) - Alerting Signals and Tones (5.5) - DSN Transmission (6) - IDLC (7.5) - ISDN Generic Requirements (10) - Timing Modes (11.1) - Synchronization performance monitoring criteria (11.2) - DS1 traffic interfaces (11.3) - DS0 Traffic interconnects (11.4) - Reliability (12) - Security (13)	- PCM-24/PCM-30 Interoperation (7.3)		- Data Retention (9.5.2) - Auto Controls (9.6.1) - Overload Controls (9.6.2) - Manual Controls (9.6.3) - Treatment options (9.6.4) - Remote Access (9.7) - AMA (9.8)	

End Office (EO) Switch				
Switch	**Trunk**	**Line**	**NM**	**Attendant**
Notes: 1. Above features show title description and GSCR paragraph (in brackets).				

Small End Office (SMEO) Switch				
Switch	**Trunk**	**Line**	**NM**	**Attendant**
	Interface			
	- T1 CAS DTMF - T1 CAS DP - E1 CAS MF R1 (Europe only) - E1 CAS DTMF (Europe only) - E1 CAS DP (Europe only) - T1 ISDN PRI T1.619a - T1 ISDN PRI NI-2	- 2W Analog - ISDN BRI NI-1/NI-2 - ISDN BRI T1.619a	- Ethernet TCP/IP - Serial RS-232 - X.25 or BX.25	
Feature/Capability				
- Code Restriction & Diversion (2.1.4) - Public Safety Features (2.4) - Trunk Group -make busy (2.5.5) - Trunk Group- Make Idle (2.5.6) - Carrier Group Alarms (2.5.7) - Assured Dial Tone (2.9) - DSN hotline service (2.12) - MLPP (3.1) - Preemption in the Network (3.2) - Precedence Call Diversion (3.3)	- ISDN NI 1/2 PRI (2.3.4) - CAS MLPP (3.4.1) - PRI MLPP (3.4.2) - ISDN MLPP PRI (3.7) - DSN IST Call Processing (4.4) - DSN switch outpulsing (4.5.2) - Trunk Supervisory Signaling (5.3) - Control Signaling (5.4) - ISDN DSS1 (5.7) - PCM-24 (7.1) - PCM-30 (7.2) (Europe only) - PCM-24/PCM-30 Interoperation (7.3)	- DN Identification (2.1.1) - ISDN NI 1/2 BRI (2.3.3) - Analog Line (2.3.5) - Analog Line MLPP (3.5) - ISDN MLPP BRI (3.6) - 2W User Access (4.3.3) - Analog Line termination (4.3.4) - Line Signaling (5.2)	- Data Collection (3.14) - NTMOS (9.1) - Common Data Requirements (9.2.1) - Cct Switched Net. Measurements (9.2.2) - ISDN Measurements (9.2.4) - Traffic Capacity (9.2.5) - Configuration Mgmt (9.3) - Fault Management (9.4) - AMA CDR (9.5.1) - Remote Access (9.7) - AMA (9.8)	

Small End Office (SMEO) Switch				
Switch	**Trunk**	**Line**	**NM**	**Attendant**
- Call Treatments (4.1) - Primary & Alternate Routing (4.2) - WWNDP (4.5.1) - Standard DNs (4.5.3) - Base Services - Abbrev. No. (4.5.5) - Digit Reception (4.5.6) - Digit Registration Capacity (4.5.7) - Screening (4.5.8) - Network Power (5.1) - Alerting Signals and Tones (5.5) - DSN Transmission (6) - IDLC (7.5) - ISDN Generic Requirements (10) - Timing Modes (11.1) - Reliability (12) - Security (13)				
Notes: 1. Above features show title description and GSCR paragraph (in brackets).				

<table>
<tr><th colspan="5">Private Branch Exchange (PBX) 1 - MLPP</th></tr>
<tr><th>Switch</th><th>Trunk</th><th>Line</th><th>NM</th><th>Attendant</th></tr>
<tr><td rowspan="2"></td><th colspan="4">Interface</th></tr>
<tr><td>- T1 ISDN PRI T1.619a
- T1 ISDN PRI NI-2</td><td>- 2W Analog
- ISDN BRI NI-1/NI-2
- ISDN BRI T1.619a</td><td>- Ethernet TCP/IP
- Serial RS-232
- X.25 or BX.25</td><td></td></tr>
<tr><th colspan="5">Feature/Capability</th></tr>
<tr><td>- MLPP (3.1)
- Preemption in the Network (3.2)
- Precedence Call Diversion (3.3)
- Call Treatments (4.1)
- WWNDP (4.5.1)
- Digit Reception (4.5.6)
- Alerting Signals and Tones (5.5)
- DSN Transmission (6)
- ISDN Generic Requirements (10)
- Timing Modes (11.1)
- Reliability (12)
- Security (13)</td><td>- ISDN NI 1/2 PRI (2.3.4)
- PRI MLPP (3.4.2)
- ISDN MLPP PRI (3.7)
- Trunk Supervisory Signaling (5.3)
- ISDN DSS1 (5.7)
- PCM-24 (7.1)</td><td>- DN Identification (2.1.1)
- ISDN NI 1/2 BRI (2.3.3)
- Analog Line (2.3.5)
- Analog Line MLPP (3.5)
- ISDN MLPP BRI (3.6)
- 2W User Access (4.3.3)
- Analog Line termination (4.3.4)
- Line Signaling (5.2)</td><td></td><td></td></tr>
<tr><td colspan="5">Notes:
1. Above features show title description and GSCR paragraph (in brackets).</td></tr>
</table>